RECEIVED
CENTRAL FAX CENTER
OCT 27 2003
OFFICIAL

CERTIFICATE OF TRANSMISSION
37 CFR 1.8(d)

I hereby certify that this paper or fee is being transmitted by facsimile to: Mail Stop Patent Applications-Continuation, Commissioner for Patents, P.O. Box 1450, Arlington, VA 22313-1450, facsimile number 1-703-746-7238 on this the 27th day of October, 2003

Kathryn Manes
Signature

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
SARVAR PATEL
ZULFIKAR AMIN RAMZAN

Serial No.: Unknown

Filing Date: October 27, 2003

For: EFFICIENT HASHING METHOD

Prior Serial No.: 09/175,178

Prior Filing Date: October 20, 1998

Prior Group Art Unit: 2132

Prior Examiner: Meislahn, Douglas J.

Atty. Dkt. No.: 2100.001100
Patel-13-1

PRELIMINARY AMENDMENT

On October 2, 2001, the Examiner issued a final rejection of application number 09/175,178. Applicants have filed a continuing application and submit this preliminary amendment in response to the rejections set forth in the official action of October 2, 2001.

Claim 1 was "rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier teachings of square hash of Jeuneman." In particular, the Examiner notes that "there is no rationale within [the] specification as to why [the prime number being one prime above the upper limit of Jeuneman's square hash recommendations] would be a major improvement over [the] prior art." Applicants are unaware of any statutory or case law basis for the Examiner's suggestion that a "major improvement" over the prior art must be present to warrant patentability. Rather, section 103 speaks only to the "obviousness" of the claimed invention over the prior art.

Applicants respectfully disagree with the Examiner's suggestion that using the prime $p > 2^n$ would not be an unobvious improvement over Jeuneman's function. Applicants respectfully disagree. Using prime $p > 2^n$, as Applicants have described and claimed, yields the following universal hash properties, which may not be obtained with Jeuneman's method:

$H_a(x) = (x + a)^2 \bmod p$ is a Δ-Universal hash (Theorem 1 in Reference1[1]) and
$H_a(x) = (x + a)^2 \bmod p \bmod 2^l$ is a ε-Δ-universal hash with a small $\varepsilon=3/(2^l)$ (Theorem 6 in Reference1) where 'l' < n.

The definitions of Δ-universal and ε-Δ-universal hash functions are provided in Definition 2 in Reference1 and are summarized here: when two different inputs x and y are given to the Δ-universal hash function, the probability, taken over the keys 'a', that their difference equals any value 'c' is always less than 1/p. That is for $x \neq y$, and any c, $Pr_a[(h(x) - h(y) = c] <= 1/p$.

When p is a prime number less than $2^n - 1$, as used by Jeuneman's method (or 2^m-1 in Jeuneman's notations), then it can be shown that the $(x + a)^2 \bmod p$ is never a Δ-universal hash function and $(x+a)^2 \bmod p \bmod 2^l$ is not a ε-Δ-universal for any value less than one. That is, in the case of Jeuneman's method an x,y,c value exists for which the probability that the difference of the hash output equals a specific constant is 1, in violation of the Δ-universal hash property.

For example, where m=4, 2^m=16, and a prime number less than 2^m-1 is 13; also use x=1 and y = 14 and c=0, then:

[1] Mark Etzel, Sarvar Patel, and Zulfikar Ramzan, "Square Hash: Fast Message Authentication Via Optimized Universal Hash Functions," Proc. of Crypto 1999, pp. 234-251. Online version at http://theory.lcs.mit.edu/~zulfikar/papers/sqhashfinal1.ps

$$
\begin{aligned}
&P_a[h(x)-h(y)=c] \\
&= P_a[(x+a)^2 - (y+a)^2 = c \bmod p] \\
&= P_a[(1+a)^2 - (14+a)^2 = 0 \bmod 13] \\
&= P_a[(1 \bmod 13 + a)^2 - (14 \bmod 13 + a)^2 = 0 \bmod p] \\
&= P_a[(1 + a)^2 - (1+a)^2 = 0 \bmod p] \\
&= P_a[0 = 0] = 1
\end{aligned}
$$

Thus with Jeuneman's method $(x+a)^2 \bmod p$ is never a Δ-universal hash function but with Applicants' method it always is, as proved in Reference1.

Accordingly, Applicants submit that the prior art fails to teach or suggest using a prime number p greater than 2^n. Moreover, the prior art does not recognize the significant advantages arising from this feature, and thus no reason to modify the teachings of the prior art exists. Accordingly, Applicants respectfully request that the rejection be withdrawn and that claim 1 be allowed.

Claim 2 was "rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier teachings of square hash of Jeuneman in view of Takaragi." Takaragi was apparently cited for the principle of "adding constants" to the square hash of Jeuneman. Takaragi, however, never teaches or suggests the use of a prime number $p > 2^n$, which, like claim 1 discussed above, is also set forth in claim 2. Thus, Takaragi does nothing to cure the fundamental deficiency of Schneier in view of Jeuneman. Accordingly, claim 2 is patentably distinct over the prior art for the same reasons discussed above in conjunction with claim 1, and Applicants respectfully request that the rejection be withdrawn and claim 2 be allowed.

Claim 3 was "rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier teachings of square hash of Jeuneman in view of Rohatgi ..., further in view of Bellare and

Received from < 7139347011 > at 10/27/03 5:02:03 PM [Eastern Standard Time]

Micciancio Eurocrypty 97 Proceedings." Neither Rohatgi or Bellare and Micciancio teaches or suggests the use of a prime number $p > 2^n$, which, like claim 1 discussed above, is also set forth in claim 3. Thus, Rohatgi or Bellare and Micciancio do nothing to cure the fundamental deficiency of Schneier in view of Jeuneman. Accordingly, claim 3 is patentably distinct over the prior art for the same reasons discussed above in conjunction with claim 1, and Applicants respectfully request that the rejection be withdrawn and claim 3 be allowed.

Respectfully submitted,

23720
PATENT TRADEMARK OFFICE

Terry D. Morgan
Reg. No. 31,181

Attorney for Applicants

WILLIAMS, MORGAN & AMERSON
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-4050

Date: October 27, 2003

RECEIVED
CENTRAL FAX CENTER
OCT 27 2003
OFFICIAL